COMPUTING CONJUGATING SETS AND AUTOMORPHISM GROUPS OF RATIONAL FUNCTIONS

XANDER FABER, MICHELLE MANES, AND BIANCA VIRAY

Abstract. Let ϕ and ψ be endomorphisms of the projective line of degree at least 2, defined over a field F. From a dynamical perspective, a significant question is to determine whether ϕ and ψ are conjugate (or to answer the related question of whether a given rational function ϕ has a nontrivial automorphism). We construct efficient algorithms for computing the set of conjugating maps (resp., the group of automorphisms), with an emphasis on the case where F is a finite field or a number field. Each of our algorithms takes advantage of different dynamical structures, so context (e.g., field of definition and degree of the map) determines the preferred algorithm.

1. Introduction

Let F be a field, and let $\phi = f/g \in F(z)$ be a rational function, where f, g are relatively prime polynomials. Unless otherwise specified, we assume throughout that

$$d = \deg(\phi) := \max\{\deg(f), \deg(g)\} \geq 2.$$

When viewed as an endomorphism of the projective line $\mathbb{P}^1_F \xrightarrow{\phi} \mathbb{P}^1_F$, a dynamical theory of ϕ arises from iteration. That is, for $x \in \mathbb{P}^1(F)$, we may consider its orbit

$$x \mapsto \phi(x) \mapsto \phi^2(x) \mapsto \phi^3(x) \mapsto \cdots$$

(Here we write $\phi^1 = \phi$ and $\phi^n = \phi \circ \phi^{n-1}$ for each $n > 1$.)

Two rational functions $\phi, \psi \in F(z)$ are *conjugate* if there is some rational function f of degree 1 (an automorphism of $\mathbb{P}^1$) defined over $\overline{F}$, an algebraic closure of F, such that $f \circ \phi = \psi \circ f$. In this case, the two functions exhibit the same *geometric* dynamical behavior. Indeed, if $f \in \overline{F}(z)$ conjugates ϕ to ψ, then f maps the ϕ-orbit of a point $x \in \mathbb{P}^1(\overline{F})$ to the ψ-orbit of $f(x)$. We say that ϕ and ψ are conjugate over a field extension E/F if they satisfy the relation $f \circ \phi = \psi \circ f$ for some rational function $f \in E(z)$ of degree 1. In this case, they have the same *arithmetic* dynamical behavior over E; e.g., f maps ϕ-orbits of E-rational points to ψ-orbits of E-rational points, and the field extension of E generated by the period-n points of ϕ and ψ must agree for every $n \geq 1$.

Conversely, given two functions that seemingly exhibit the same dynamical behavior, one wants to know if they are conjugate, or if there is some deeper structure that should be investigated. This natural question sparked the current work, in which we study the following pair of algorithmic problems:

Date: September 26, 2014.

2010 *Mathematics Subject Classification.* 37P05 (primary); 11Y16 (secondary) .

The first and second authors were partially supported by NSF grants DMS-0902532 and DMS-1102858, respectively. The third author was partially supported by NSF grant DMS-1002933 and by ICERM.

(1) For two rational functions ϕ and ψ, determine the set of rational functions f of degree 1 (automorphisms of $\mathbb{P}^1$) that conjugate ϕ to ψ, i.e., such that $f \circ \phi \circ f^{-1} = \psi$.

(2) For a given rational function ϕ, determine the **automorphism group of** ϕ; i.e., determine the set of rational functions f of degree 1 such that $f \circ \phi \circ f^{-1} = \phi$.

These two questions are intimately connected. In §2 we show that the set of automorphisms can be viewed as the points of a finite group scheme, denoted Aut_ϕ. In §3 we show that the set of maps conjugating ϕ to ψ is also a scheme, denoted $\mathrm{Conj}_{\phi,\psi}$, which is a principal homogeneous space for Aut_ϕ. In particular, conjugacy over F and conjugacy over an algebraic closure $\overline{F}$ are equivalent notions whenever ϕ (and ψ) has trivial automorphism group. More generally, one can show that the size of the automorphism group of ϕ (or ψ) bounds the degree of the field extension generated by the coefficients of any conjugating map [LMT12].

The symmetry locus of rational functions — the space of rational functions with nontrivial automorphism group — can be thought of as an analogue of the locus of abelian varieties that have extra automorphisms. Indeed, just as the presence of elliptic curves with extra automorphisms obstructs the existence of a universal elliptic curve, so does the symmetry locus obstruct the existence of a fine moduli space of conjugacy classes of rational functions. The algorithms discussed below may be viewed as a computational tool for detecting if a given rational function is an obstruction.

Algorithms. We provide algorithms in §4, §5, and §6 that take advantage of dynamical structure to compute the field-valued points of Aut_ϕ and $\mathrm{Conj}_{\phi,\psi}$. Each algorithm utilizes different types of dynamical structure, and consequently each has its own strengths and weaknesses. In §8, we briefly describe two additional algorithms, which are "naive" in the sense that they do not take advantage of context-specific knowledge. We describe these two algorithms mainly for the sake of completeness and for performance comparison.

By way of a disclaimer, we have attempted to stress concept and clarity in our algorithms; we have not endeavored to explain all of the small tricks we used at the level of implementation. This is especially true in Algorithm 2, the Chinese Remainder Theorem. We refer the interested reader to our source code which is included with the `arXiv` distribution of this article.

Method of Invariant Sets. This algorithm computes the absolute conjugating set (defined over an algebraic closure $\overline{F}$) using linear algebra, based on the existence of a pair of subsets $T_\phi, T_\psi \subset \mathbb{P}^1(\overline{F})$ such that $f(T_\phi) = T_\psi$ for all $f \in \mathrm{Conj}_{\phi,\psi}(\overline{F})$. A descent trick allows one to rapidly determine which elements of $\mathrm{Conj}_{\phi,\psi}(\overline{F})$ are F-rational. The same method can be used to compute the absolute and F-rational automorphism groups. See §4.

Chinese Remainder Theorem. When $F = \mathbb{Q}$, we give an arithmetically motivated algorithm to compute $\mathrm{Conj}_{\phi,\psi}(\mathbb{Q})$ (or $\mathrm{Aut}_\phi(\mathbb{Q})$). First we compute $\mathrm{Conj}_{\phi,\psi}(\mathbb{F}_p)$ for a number of primes p (by exhaustive search or any of our other methods), and then we glue this information together using the Chinese Remainder Theorem (CRT). To show that this algorithm terminates, we prove that the heights of the elements in $\mathrm{Conj}_{\phi,\psi}(\mathbb{Q})$ are bounded in terms of the coefficients of ϕ and ψ. See §5, where we also work over an arbitrary number field.

Method of Fixed Points. The action of ϕ on the fixed points of a nontrivial element $f \in \mathrm{Aut}_\phi(F)$ is highly restricted, both geometrically and arithmetically. We exploit this restriction to develop another algorithm for computing $\mathrm{Aut}_\phi(F)$. See §6.

Gröbner Bases. Since $\mathrm{Conj}_{\phi,\psi}$ and Aut_ϕ are zero-dimensional schemes naturally defined by $2d+1$ homogeneous polynomials of degree $d+1$ in four variables, one may apply standard Gröbner basis techniques to compute the points of $\mathrm{Conj}_{\phi,\psi}$ or Aut_ϕ. See §7.1.

Exhaustive Search. When ϕ and ψ are defined over a finite field $\mathbb{F}_q$, one could, in theory, determine $\mathrm{Conj}_{\phi,\psi}(\mathbb{F}_q)$ or $\mathrm{Aut}_\phi(\mathbb{F}_q)$ by exhaustive search. This computation is feasible when the degrees of ϕ, ψ and the size of the finite field are reasonably small. See §7.2.

Comparison of algorithms. In §8 we compare the running times of the algorithms for computing $\mathrm{Aut}_\phi(\mathbb{Q})$ for a large number of randomly generated rational functions of various degrees and various heights, and also for rational functions with nontrivial automorphism group. See Tables 1, 2, and 3 for precise timings.

The running times for random maps demonstrate that the method of fixed points is preferable to the CRT method for rational functions of degree up to about 12, when the two methods become comparable. For larger degrees, the CRT method is preferable. As a benchmark, we compare our new algorithms with the Gröbner basis algorithm. Our experiments show that this naive method is comparable with the fixed point method when the degree is two or three, but on average performs an order of magnitude worse already for functions of degree 6 and two orders of magnitude worse for functions of degree 9.

The method of invariant sets is not competitive with the other algorithms on random maps, as these tend to require computations in number fields of large degree. It compares favorably and occasionally better for maps with nontrivial automorphisms. We stress, however, that the main advantage the method of invariant sets has over the other algorithms is that it computes the $\overline{F}$-rational conjugation maps and automorphisms. In particular, this means it can detect if a function lies is in the symmetry locus.

It is worth noting that modern research on the dynamics of rational functions often focuses on low degree, with an abundance of open questions even in degrees 2 (see, for example, [Mil93, Poo98]) and 3 (see [Mil09]). So there is already ample room for generating, testing, and refining new conjectures on rational functions of degrees between 3 and 10, say, and we believe the tools presented here will be useful in this regard.

Acknowledgements. This project began at the University of Georgia, during an NSF–sponsored summer school on Arithmetic Dynamics. We thank the organizer, Robert Rumely, for the experience, and Rafe Jones for inspiring this work with a comment during one of his talks. The authors are grateful for the opportunity to complete the project at the Institute for Computational and Experimental Research in Mathematics. We thank the anonymous referees for their comments, and give special thanks to Joseph H. Silverman for helpful comments on our number field algorithm.

2. The automorphism scheme

Let R be a noetherian commutative ring with unity, and let R-**Alg** and **Grp** denote the categories of commutative R-algebras and (abstract) groups, respectively. For any R-algebra S, we identify $\mathrm{PGL}_2(S)$ with $\mathrm{Aut}(\mathbb{P}^1_S)$, the group of automorphisms of $\mathbb{P}^1$ defined over S. We make the following definition:

Definition. Let $\phi : \mathbb{P}^1_R \to \mathbb{P}^1_R$ be a morphism of degree at least 2. Let $\underline{\mathrm{Aut}}_\phi$ denote the functor from R-**Alg** $\to$ **Grp** given by

$$S \mapsto \{f \in \mathrm{Aut}(\mathbb{P}^1_S) : \phi = f \circ \phi \circ f^{-1}\}.$$

The functor $\underline{\mathrm{Aut}}_\phi$ acts on R-algebra morphisms by base extension of the associated group of automorphisms.

The remainder of this section will be devoted to showing that the functor $\underline{\mathrm{Aut}}_\phi$ is represented by a finite group scheme.

Theorem 2.1. *Let R be a noetherian commutative ring and let $\phi : \mathbb{P}^1_R \to \mathbb{P}^1_R$ be an endomorphism of degree at least 2. Then the functor $\underline{\mathrm{Aut}}_\phi$ is represented by a closed finite R-subgroup scheme $\mathrm{Aut}_\phi \subset \mathrm{PGL}_2$.*

Remark 2.2. The group scheme Aut_ϕ need not be flat over $\mathrm{Spec}\, R$. For example, if $\phi(z) = z^2$ is an endomorphism of the projective line over $\mathbb{Z}_2$, then there is nontrivial 2-torsion in the ring of global functions of Aut_ϕ. Intuitively, this is because $\mathrm{Aut}_\phi(\overline{\mathbb{Q}_2}) = \{z, 1/z\}$, while $\mathrm{Aut}_\phi(\overline{\mathbb{F}}_2) \cong \mathrm{PGL}_2(\mathbb{F}_2)$, which has order 6.

The proof of the theorem will be postponed until §2.2. Our main contribution lies in showing that Aut_ϕ is proper over $\mathrm{Spec}\, R$. The Reduction Lemma, stated and proved in the next subsection, will allow us to prove properness, and it will also be a key tool in the Chinese Remainder Theorem algorithm detailed in §5.

2.1. **Properness.**

If k is a non-Archimedean field (not necessarily complete) with valuation ring $\mathfrak{o}$, we say that an endomorphism $\phi : \mathbb{P}^1_k \to \mathbb{P}^1_k$ has **good reduction** if there exists a morphism $\Phi : \mathbb{P}^1_{\mathfrak{o}} \to \mathbb{P}^1_{\mathfrak{o}}$ that agrees with ϕ on the generic fiber.

Reduction Lemma. *Let k be a non-Archimedean field with valuation ring $\mathfrak{o}$ and residue field $\mathbb{F}$, and let $\phi \in k(z)$ be a rational function of degree at least 2 (which is equivalent to a morphism $\mathbb{P}^1_k \to \mathbb{P}^1_k$). Suppose that ϕ has good reduction. Then every element of $\underline{\mathrm{Aut}}_\phi(k)$ has good reduction, and the canonical reduction $\mathfrak{o} \to \mathbb{F}$ induces a homomorphism* $\mathrm{red} : \underline{\mathrm{Aut}}_\phi(k) \to \underline{\mathrm{Aut}}_\phi(\mathbb{F})$. *If $\mathbb{F}$ has characteristic $p > 0$ (resp. characteristic zero), then the kernel of reduction is a p-group (resp. trivial).*

The proof of the Reduction Lemma uses dynamics on the Berkovich projective line. For a comprehensive background, see [BR10]. For a more concise summary of the ideas used here, we direct the reader to [Fab13].

Proof. Let $\mathbb{C}_k$ be a minimal complete and algebraically closed non-Archimedean extension of k, and let $\mathbf{P}^1$ be the Berkovich analytification of the projective line $\mathbb{P}^1_{\mathbb{C}_k}$. The morphism ϕ extends functorially to $\mathbf{P}^1$. We use two key facts due to Rivera-Letelier [RL05, Thm. 4]:

1. a rational function f has good reduction if and only if the Gauss point $\zeta \in \mathbf{P}^1$ is totally invariant; i.e., $f^{-1}(\zeta) = \{\zeta\}$, and
2. a rational function of degree at least 2 has at most one totally invariant point in $\mathbf{P}^1 \smallsetminus \mathbb{P}^1(\mathbb{C}_k)$.

For $f \in \underline{\mathrm{Aut}}_\phi(k)$, we have

$$f^{-1}(\zeta) = f^{-1}(\phi^{-1}(\zeta)) = (\phi \circ f)^{-1}(\zeta) = (f \circ \phi)^{-1}(\zeta) = \phi^{-1}(f^{-1}(\zeta)).$$

Hence $f^{-1}(\zeta)$ is a totally invariant point for ϕ, so that $f(\zeta) = \zeta$. Equivalently, f has good reduction. Thus the reduction map $\mathrm{red} : \underline{\mathrm{Aut}}_\phi(k) \to \underline{\mathrm{Aut}}_\phi(\mathbb{F})$ is well-defined, and it is evidently a homomorphism.

Now we compute the kernel of reduction. Suppose $\mathrm{red}(f)$ is trivial. Without loss of generality, we may replace k with a finite extension in order to assume that f has a k-rational fixed point. Moreover, we may conjugate f by an element of $\mathrm{PGL}_2(\mathfrak{o})$ in order to assume that $f(\infty) = \infty$, so $f(z) = \alpha z + \beta$.

Silverman has shown that $\underline{\mathrm{Aut}}_\phi(L)$ is a finite group for any algebraically closed field L [Sil07, Prop. 4.65][1], so f necessarily has finite order $m \geq 1$. The equation $f^m(z) = z$ shows that α is an m-th root of unity. But $\mathrm{red}(f)$ is trivial, so the image of α in the residue field $\mathbb{F}$ is 1. If k has residue characteristic zero, then we conclude that $\alpha = 1$ and $\beta = 0$. Otherwise, we find that α is a p-power root of unity in k, and hence f has p-power order in $\underline{\mathrm{Aut}}_\phi(k)$. □

Remark 2.3. A different proof of the first part of the Reduction Lemma can be given using the maximum modulus principle in non-Archimedean analysis [PST09, Lem. 6].

Proposition 2.4. *Let F be a field, and let $n \geq 2$ be an integer. Suppose that $\phi : \mathbb{P}^1_F \to \mathbb{P}^1_F$ is a morphism of degree $d \geq 2$ such that $\underline{\mathrm{Aut}}_\phi(F)$ contains an element of order n. Then n divides one of d, $d-1$, or $d+1$.*

Proof. We may assume without loss of generality that F is algebraically closed. Let $s \in \underline{\mathrm{Aut}}_\phi(F)$ have order n. We conjugate one of the fixed points of s to ∞, so that $s = \left(\begin{smallmatrix} \alpha & \beta \\ 0 & 1 \end{smallmatrix}\right)$. (Note that replacing s with usu^{-1} has the effect of replacing ϕ with $u\phi u^{-1}$.) The proof divides into two cases, depending on whether $\alpha = 1$ or $\alpha \neq 1$.

If $\alpha = 1$, then s has only one fixed point, and $n = \mathrm{char}(F)$ is necessarily prime.

Replace s with $\left(\begin{smallmatrix} \beta^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right) s \left(\begin{smallmatrix} \beta & 0 \\ 0 & 1 \end{smallmatrix}\right)$ in order to assume that $\beta = 1$. It follows that $\phi(z+1) - 1 = \phi(z)$, or equivalently, that the function $\phi(z) - z$ is invariant under the map $z \mapsto z+1$. Hence there exists a rational function $\psi(z) \in F(z)$ such that $\phi(z) - z = \psi(z^n - z)$. We conclude that $\deg(\phi) = n \cdot \deg(\psi)$ or $n \cdot \deg(\psi) + 1$.

Now suppose that $\alpha \neq 1$, so s has two distinct fixed points: ∞ and $\beta/(1-\alpha)$. We may conjugate the second fixed point to 0 in order to assume that $\beta = 0$. Note that this implies that $\alpha \in F^\times$ has multiplicative order n. To say that s is an automorphism of ϕ is equivalent to saying that $\phi(z)/z$ is invariant under the map $z \mapsto \alpha z$. Hence there is a rational function $\psi \in F(z)$ such that $\phi(z)/z = \psi(z^n)$. So $\deg(\phi) = n \cdot \deg(\psi)$ or $n \cdot \deg(\psi) \pm 1$. □

The Reduction Lemma yields an injectivity statement for reduction of automorphisms at all but finitely many places of a number field. For notation, if K is a number field and v is a finite place of K, we write K_v and $\mathbb{F}_v$ for the completion of K at v and the residue field of K_v, respectively. If $\phi \in K(z)$ is a rational function, we say that it has **good reduction at** v if the induced rational function over K_v has good reduction in the above sense. (Equivalently, ϕ has good reduction at v if one can reduce its coefficients modulo v, and the resulting endmorphism of $\mathbb{P}^1_{\mathbb{F}_v}$ has the same degree as ϕ.)

Proposition 2.5. *Let K be a number field and let $\phi \in K(z)$ be a rational function of degree $d \geq 2$. Define S_0 to be the set of rational primes given by*

$$S_0 = \{2\} \cup \left\{ p \textit{ odd} : \frac{p-1}{2} \Big| [K : \mathbb{Q}] \ \textit{ and } \ p \mid d(d^2-1) \right\},$$

[1] Alternatively, §4 gives a conceptually simpler proof of Silverman's result.

and let S be the (finite) set of places of K of bad reduction for ϕ along with the places that divide a prime in S_0. Then $\mathrm{red}_v : \underline{\mathrm{Aut}}_\phi(K) \to \underline{\mathrm{Aut}}(\mathbb{F}_v)$ is a well defined injective homomorphism for all finite places v outside S.

Proof. By the Reduction Lemma, it suffices to prove that if $v \notin S$, then $\underline{\mathrm{Aut}}_\phi(K)$ has no element of order p, where $v \mid p$. Suppose otherwise.

The group $\mathrm{PGL}_2(\mathbb{C})$ contains a unique subgroup of order p, up to conjugation, so that an element of order p is conjugate to $\left(\begin{smallmatrix} \zeta_p & 0 \\ 0 & \zeta_p^{-1} \end{smallmatrix}\right)$. Taking traces shows that $\zeta_p + \zeta_p^{-1} \in K$. Note that $[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] = \frac{1}{2}(p-1)$ for $p > 2$, so that $\frac{p-1}{2} \mid [K : \mathbb{Q}]$. If $\underline{\mathrm{Aut}}_\phi(K)$ contains an element of order p, then p divides $d(d^2-1)$ by Proposition 2.4. Hence $p \in S_0$, and so $v \in S$. □

Proposition 2.5 often allows one to determine the group structure of $\underline{\mathrm{Aut}}_\phi(K)$ very quickly by computing $\underline{\mathrm{Aut}}_\phi(\mathbb{F}_v)$ for a few places $v \notin S$. This is analogous to the way one typically computes the torsion subgroup of an elliptic curve over a number field; see [Sil09, VII.3]. (If one wishes to compute the *elements* of $\mathrm{Aut}_\phi(K)$ rather than just the group structure, then more work is required.)

2.2. **Proof of Theorem 2.1.** Fix a noetherian commutative ring R. Over R, PGL_2 may be embedded as an affine subvariety of $\mathbb{P}^3_R = \mathrm{Proj}\ R[\alpha, \beta, \gamma, \delta]$; indeed, it is the complement of the quadric $\alpha\delta - \beta\gamma = 0$. Let $\phi : \mathbb{P}^1_R \to \mathbb{P}^1_R$ be a nonconstant endomorphism. We may define Aut_ϕ as a subgroup scheme of PGL_2 as follows. After fixing coordinates of $\mathbb{P}^1_R$, the morphism ϕ can be given by a pair of homogeneous polynomials $\Phi = (\Phi_0(X,Y), \Phi_1(X,Y))$ of degree $d = \deg(\phi)$ with coefficients in R such that the homogeneous resultant $\mathrm{Res}(\Phi_0, \Phi_1)$ is a unit in R. The pair Φ_0, Φ_1 is unique up to multiplication by a common unit in R. Similarly, for any R-algebra S, an element $f \in \mathrm{PGL}_2(S)$ may be given by a pair

$$F = (\alpha X + \beta Y, \gamma X + \delta Y), \qquad \text{with } \alpha, \beta, \gamma, \delta \in S \text{ and } \alpha\delta - \beta\gamma \in S^\times.$$

Note that f^{-1} is represented by the pair $F^{-1} := (\delta X - \beta Y, -\gamma X + \alpha Y)$. Then $f \circ \phi \circ f^{-1} = \phi$ is equivalent to saying that $F \circ \Phi \circ F^{-1}$ and Φ define the same morphism on $\mathbb{P}^1_S \to \mathbb{P}^1_S$. If we define $(\Phi_0'(X,Y), \Phi_1'(X,Y)) = F \circ \Phi \circ F^{-1}$, then this is equivalent to

$$\Phi_0(X,Y)\Phi_1'(X,Y) - \Phi_1(X,Y)\Phi_0'(X,Y) = 0. \tag{2.1}$$

The expression on the left is a homogeneous polynomial of degree $2d$ in X and Y whose coefficients are homogeneous polynomials in $R[\alpha, \beta, \gamma, \delta]$. So (2.1) gives $2d+1$ equations that cut out a closed subscheme of PGL_2 defined over R. One checks readily that $\mathrm{Aut}_\phi(S)$ is a subgroup of $\mathrm{PGL}_2(S)$ for every S.

Next we argue that Aut_ϕ is a finite group scheme over R when ϕ has degree at least 2. The map $\mathrm{Aut}_\phi \to \mathrm{Spec}\, R$ is quasi-finite. Indeed, it suffices to check this statement on geometric fibers, and it is known that $\mathrm{Aut}_\phi(L)$ is a finite group for any algebraically closed field L [Sil07, Prop. 4.65].

Moreover, Aut_ϕ is proper over $\mathrm{Spec}\, R$. Indeed, since Aut_ϕ and $\mathrm{Spec}\, R$ are noetherian, this can be checked using the valuative criterion for properness using only discrete valuation rings [Har77, Ex. II.4.11]. Let $\mathfrak{o}$ be a discrete valuation ring with field of fractions k, and consider a commutative diagram

$$\begin{tikzcd}
\operatorname{Spec} k \arrow[r] \arrow[d] & \mathrm{Aut}_\phi \arrow[d] \\
\operatorname{Spec} \mathfrak{o} \arrow[r] \arrow[ur, dashed] & \operatorname{Spec} R.
\end{tikzcd}$$

The left vertical map is the canonical open immersion, and the right vertical map is the structure morphism. We must show there is a unique morphism $\operatorname{Spec} \mathfrak{o} \to \mathrm{Aut}_\phi$ that makes the entire diagram commute. Without loss of generality, we may assume that $R = \mathfrak{o}$ and that the lower horizontal arrow is the identity map.

If $v : k \to \mathbb{Z} \cup \{+\infty\}$ is the canonical extension of the valuation on $\mathfrak{o}$, then we may endow k with the structure of a non- Archimedean field by setting $|x| = e^{-v(x)}$ for every $x \in k$. (Note that we interpret $e^{-\infty}$ as zero.) Since ϕ is defined over $\mathfrak{o}$, it has good reduction. The Reduction Lemma asserts that every k-automorphism of ϕ also has good reduction. Equivalently, every k-valued point may be extended to an $\mathfrak{o}$-valued point, which is what we wanted to show.

We now know that $\mathrm{Aut}_\phi \to \operatorname{Spec} R$ is a quasi-finite proper morphism. Zariski's main theorem tells us that it factors as an open immersion of R-schemes $\mathrm{Aut}_\phi \to X$ followed by a finite morphism $X \to \operatorname{Spec} R$. But Aut_ϕ is proper, so any open immersion is actually an isomorphism. Hence Aut_ϕ is finite over $\operatorname{Spec} R$.

3. The conjugation scheme

As in the previous section, we let R be a noetherian commutative ring with 1, and we consider rational functions $\phi, \psi : \mathbb{P}^1_R \to \mathbb{P}^1_R$ of degree $d \geq 2$. The development of the R-scheme of rational functions of degree 1 conjugating ϕ to ψ proceeds along similar lines as the construction of the scheme Aut_ϕ in the previous section. We will be content to state the results and only sketch the major differences here.

Definition. Fix an integer $d \geq 2$, and let $\phi, \psi : \mathbb{P}^1_R \to \mathbb{P}^1_R$ be two endomorphisms of degree d. Write **Set** for the category of sets. Let $\underline{\mathrm{Conj}}_{\phi,\psi} : R$-**Alg** $\to$ **Set** denote the functor given by

$$\underline{\mathrm{Conj}}_{\phi,\psi}(S) = \{f \in \mathrm{Aut}(\mathbb{P}^1_S) : f \circ \phi \circ f^{-1} = \psi\}.$$

The functor $\underline{\mathrm{Conj}}_{\phi,\psi}$ acts on R-algebra morphisms by base extension of the associated set of conjugation maps.

Theorem 3.1. *Let R be a noetherian commutative ring with 1, let $d \geq 2$ be an integer, and let $\phi, \psi : \mathbb{P}^1_R \to \mathbb{P}^1_R$ be endomorphisms of degree d. Then the functor $\underline{\mathrm{Conj}}_{\phi,\psi}$ is represented by a closed finite R-subscheme $\mathrm{Conj}_{\phi,\psi} \subset \mathrm{PGL}_2$.*

Remark 3.2. The theorem does not preclude the possibility that $\mathrm{Conj}_{\phi,\psi}$ is the empty scheme. The group scheme PGL_2 has relative dimension 3 over R, while the space Rat_d of endomorphisms of $\mathbb{P}^1$ of degree d has relative dimension $2d + 1 > 3$. So for a fixed $\phi \in \mathrm{Rat}_d(R)$, a general choice of ψ will yield $\mathrm{Conj}_{\phi,\psi} = \varnothing$.

Remark 3.3. When $\mathrm{Conj}_{\phi,\psi}$ is not the empty scheme, it is a principal homogeneous space for Aut_ϕ (and Aut_ψ). This observation will be used explicitly to show that $\mathrm{Conj}_{\phi,\psi}$ is quasi-finite.

The construction of the closed subscheme $\mathrm{Conj}_{\phi,\psi} \subset \mathrm{PGL}_2$ is similar to that of Aut_ϕ in §2, so we leave the details to the reader. Note that the equations defined by (2.1) remain equally valid in this setting if we write $\Psi = (\Psi_0(X,Y), \Psi_1(X,Y))$ for a homogenization of ψ and replace Φ_i with Ψ_i. In particular, $\mathrm{Conj}_{\phi,\psi}$ is cut out as a subscheme of PGL_2 by $2d+1$ homogeneous polynomials of degree $d+1$ in the four variables $\alpha, \beta, \gamma, \delta$, where $\mathrm{PGL}_2 \subset \mathrm{Proj}\ R[\alpha,\beta,\gamma,\delta]$.

In order to establish that $\mathrm{Conj}_{\phi,\psi}$ is finite over $\mathrm{Spec}\, R$, one must argue that it is proper and quasi-finite. Properness follows from a direct generalization of the Reduction Lemma (and its proof):

Reduction Lemma (Part II)**.** *Let k be a non-Archimedean field with valuation ring $\mathfrak{o}$ and residue field $\mathbb{F}$, and let $\phi, \psi \in k(z)$ be rational functions of degree at least 2. Suppose that both ϕ and ψ have good reduction. Then every element of $\mathrm{Conj}_{\phi,\psi}(k)$ has good reduction, and the canonical reduction $\mathfrak{o} \to \mathbb{F}$ induces a map of sets $\mathrm{red}_{\phi,\psi} : \mathrm{Conj}_{\phi,\psi}(k) \to \mathrm{Conj}_{\phi,\psi}(\mathbb{F})$. If the order of $\mathrm{Aut}_\phi(k)$ is relatively prime to the characteristic of $\mathbb{F}$, then $\mathrm{red}_{\phi,\psi}$ is injective.*

Proof. Only the final statement of the lemma requires further comment. The Reduction Lemma for Aut_ϕ shows that the kernel of the homomorphism $\mathrm{red}_\phi : \mathrm{Aut}_\phi(k) \to \mathrm{Aut}_\phi(\mathbb{F})$ is trivial. If $f, g \in \mathrm{Conj}_{\phi,\psi}(k)$ have the same image in $\mathrm{Conj}_{\phi,\psi}(\mathbb{F})$, then $f^{-1}g$ lies in the kernel of red_ϕ, so that $f = g$. □

To complete the proof of Theorem 3.1, it remains to show that $\mathrm{Conj}_{\phi,\psi}$ is quasi-finite, for which it suffices to take $R = F$ to be a field and prove that $\mathrm{Conj}_{\phi,\psi}(F)$ is finite. If $\mathrm{Conj}_{\phi,\psi}(F)$ is empty, we are finished. Otherwise, fix an element $f_0 \in \mathrm{PGL}_2(F)$ that conjugates ϕ to ψ. Given an element $f \in \mathrm{Conj}_{\phi,\psi}(F)$, we see that

$$(f_0^{-1} \circ f) \circ \phi \circ (f_0^{-1} \circ f)^{-1} = f_0^{-1} \circ \left(f \circ \phi \circ f^{-1}\right) \circ f_0 = f_0^{-1} \circ \psi \circ f_0 = \phi.$$

That is, the association $f \mapsto f_0^{-1} \circ f$ defines a map of sets

$$\mathrm{Conj}_{\phi,\psi}(F) \to \mathrm{Aut}_\phi(F),$$

which one readily verifies is a bijection. Since $\mathrm{Aut}_\phi(F)$ is a finite set, so is $\mathrm{Conj}_{\phi,\psi}(F)$.

We close this section with a version of Proposition 2.5 that applies to conjugation sets.

Corollary 3.4. *Let K be a number field and let $\phi, \psi \in K(z)$ be rational functions of degree $d \geq 2$. Define S_0 to be the set of rational primes given by*

$$S_0 = \{2\} \cup \left\{ p \text{ odd} : \frac{p-1}{2} \middle| [K : \mathbb{Q}] \text{ and } p \mid d(d^2-1) \right\},$$

and let S be the (finite) set of places of K of bad reduction for ϕ or ψ along with the places that divide a prime in S_0. If $\mathrm{Conj}_{\phi,\psi}(K)$ is nonempty, then $\mathrm{red}_v : \mathrm{Conj}_{\phi,\psi}(K) \to \mathrm{Conj}_{\phi,\psi}(\mathbb{F}_v)$ is a well defined injection of sets for all finite places v outside S.

Proof. Let $f_0 \in \mathrm{Conj}_{\phi,\psi}(K)$. For $v \notin S$, we have the following diagram of morphisms of sets.

$$\begin{tikzcd}
\mathrm{Conj}_{\phi,\psi}(K) \arrow[r, "\mathrm{red}_v"] \arrow[d, "f_0^{-1}\circ"'] & \mathrm{Conj}_{\phi,\psi}(\mathbb{F}_v) \arrow[d, "\mathrm{red}_v(f_0)^{-1}\circ"] \\
\mathrm{Aut}_\phi(K) \arrow[r, "\mathrm{red}_v"] & \mathrm{Aut}_\phi(\mathbb{F}_v)
\end{tikzcd}$$

The vertical arrows denote postcomposition with the indicated element; they are bijections by the discussion immediately preceding this proof. The Reduction Lemmas show that the horizontal arrows are well defined. The diagram commutes because PGL_2 is a group scheme. We have already shown the lower horizontal arrow is injective (Proposition 2.5), so the top one must share this property. □

4. Algorithm 1: Method of Invariant Sets

Let F be an arbitrary field, and suppose $\phi, \psi : \mathbb{P}^1_F \to \mathbb{P}^1_F$ are morphisms of degree at least 2. In this section, we describe a geometric algorithm to compute $\mathrm{Conj}_{\phi,\psi}(\overline{F})$, where $\overline{F}$ is an algebraic closure of F. (Of course, the algorithm computes $\mathrm{Aut}_\phi(\overline{F})$ when $\phi = \psi$.) More precisely, the method of invariant sets produces a finite Galois extension E/F and the set $\mathrm{Conj}_{\phi,\psi}(E) = \mathrm{Conj}_{\phi,\psi}(\overline{F})$. With some small additional work, we will also be able to compute $\mathrm{Conj}_{\phi,\psi}(F)$.

4.1. **Overview.** The key to the algorithm lies in constructing what we call an **invariant pair for ϕ and ψ**: a pair of subsets $T_\phi, T_\psi \subset \mathbb{P}^1(\overline{F})$ such that

- $\#T_\phi = \#T_\psi \geq 3$, and
- $s(T_\phi) = T_\psi$ for every $s \in \mathrm{Conj}_{\phi,\psi}(\overline{F})$.[2]

Given an invariant pair, we have

$$\mathrm{Conj}_{\phi,\psi}(\overline{F}) \subset \mathrm{Hom}_{\overline{F}}(T_\phi, T_\psi) \subset \mathrm{PGL}_2(\overline{F}).$$

For F a given field of definition for ϕ and ψ, one cannot always find the required sets T_ϕ and T_ψ in $\mathbb{P}^1(F)$, but they are always constructible over a finite extension E/F, yielding

$$\mathrm{Conj}_{\phi,\psi}(\overline{F}) = \mathrm{Conj}_{\phi,\psi}(E) \subset \mathrm{Hom}_E(T_\phi, T_\psi) \subset \mathrm{PGL}_2(E).$$

Since any element of $\mathrm{PGL}_2(E)$ is uniquely determined by its action on three points, we can use linear algebra to determine all maps carrying a set of three distinct points of T_ϕ to a set of three distinct points of T_ψ; these will be candidate elements of $\mathrm{Conj}_{\phi,\psi}(E)$. It is then a simple matter to check if the candidate s satisfies $s \circ \phi = \psi \circ s$.

4.2. **Algorithm.** We first show how to compute $\mathrm{Conj}_{\phi,\psi}(E)$ given an invariant pair defined over the field extension E/F. We also give a particular construction of an invariant pair, although certainly there are others one could use. Then we describe a simple technique for determining which elements of $\mathrm{Conj}_{\phi,\psi}(E)$ are defined over the ground field F. Finally, we briefly discuss the complexity of the algorithm.

4.2.1. *Conjugation Sets from Invariant Pairs.* Let E be any field over which ϕ and ψ are defined, and suppose that we have an invariant pair $T_\phi, T_\psi \subset \mathbb{P}^1(E)$. Algorithm 1 describes the process of computing $\mathrm{Conj}_{\phi,\psi}(E)$.

Proof of Correctness of Algorithm 1. Given $s \in \mathrm{Conj}_{\phi,\psi}(E)$, there is a triple of distinct indices $i, j, k \in \{1, \ldots, n\}$ such that

$$s(\tau_1) = \eta_i, \quad s(\tau_2) = \eta_j, \text{ and } \quad s(\tau_3) = \eta_k.$$

[2] If $\mathrm{Conj}_{\phi,\psi}(E) = \varnothing$, then the second condition is vacuous, but we will not know this a priori.

Algorithm 1 — Compute $\mathrm{Conj}_{\phi,\psi}(E)$ given an invariant pair in $\mathbb{P}^1(E)$

```
Input:
    • nonconstant rational functions $\phi, \psi \in E(z)$
    • an invariant pair $T_\phi = \{\tau_1, \dots, \tau_n\}$ and $T_\psi = \{\eta_1, \dots, \eta_n\}$ of $\mathbb{P}^1(E)$
Output: the set $\mathrm{Conj}_{\phi,\psi}(E)$
create an empty list $L$
for each triple of distinct integers $i, j, k \in \{1, \dots, n\}$:
  compute $s \in \mathrm{PGL}_2(E)$ by solving the system of linear equations
      $s(\tau_1) = \eta_i, \quad s(\tau_2) = \eta_j, \quad s(\tau_3) = \eta_k$
  if $s \circ \phi = \psi \circ s$: append $s$ to $L$
return $L$
```

Conversely, given a triple of distinct indices $i, j, k \in \{1, \dots, n\}$, there exists a unique element $s \in \mathrm{PGL}_2(E)$ such that

$$s(\tau_1) = \eta_i, \qquad s(\tau_2) = \eta_j \text{ and } \qquad s(\tau_3) = \eta_k.$$

These three equations are linear in the coefficients of s. One now determines if this candidate element s actually satisfies the functional equation

$$s \circ \phi = \psi \circ s.$$

If that is the case, then $s \in \mathrm{Conj}_{\phi,\psi}(E)$. □

4.2.2. *Constructing an Invariant Pair.* We now suppose that ϕ and ψ are conjugate rational functions defined over a field F and give a construction of an invariant pair T_ϕ and T_ψ. We may assume that $\deg(\phi) = \deg(\psi) = d$, since otherwise ϕ and ψ are not conjugate.

Let $\mathrm{Fix}(\phi)$ be the set of fixed points of ϕ, which has cardinality between 1 and $d+1$, inclusive. If $s \in \mathrm{Conj}_{\phi,\psi}(F)$ and $x \in \mathrm{Fix}(\phi)$, then

$$\psi(s(x)) = s(\phi(x)) = s(x).$$

That is, s necessarily maps $\mathrm{Fix}(\phi)$ bijectively onto $\mathrm{Fix}(\psi)$. Consequently, if the number of fixed points of ϕ differs from that of ψ, then ϕ and ψ are not conjugate.

A similar calculation shows that if $x \in \mathbb{P}^1(F)$ is any point, then s maps the set $\phi^{-n}(x)$ bijectively onto the set $\psi^{-n}(s(x))$ for each $n \geq 1$. Hence if ϕ and ψ are conjugate, it is necessary that the sets $\phi^{-n}(\mathrm{Fix}(\phi))$ and $\psi^{-n}(\mathrm{Fix}(\psi))$ have the same cardinality for each $n \geq 1$.

Define a set $T_\phi \subset \mathbb{P}^1(\overline{F})$ by the following formula:

$$T_\phi = \begin{cases} \mathrm{Fix}(\phi) & \text{if } \#\,\mathrm{Fix}(\phi) \geq 3 \\ \phi^{-1}(\mathrm{Fix}(\phi)) & \text{if } \#\,\mathrm{Fix}(\phi) = 2 \\ \phi^{-2}(\mathrm{Fix}(\phi)) & \text{if } \#\,\mathrm{Fix}(\phi) = 1. \end{cases} \tag{4.1}$$

We claim that T_ϕ has cardinality at least 3 in all cases. This is evident in the first case.

In the second case, note that $\mathrm{Fix}(\phi) \subset \phi^{-1}(\mathrm{Fix}(\phi))$. So if $\#T_\phi = \#\,\mathrm{Fix}(\phi) = 2$, then each point of $\mathrm{Fix}(\phi)$ is totally ramified for ϕ. The derivative at each of the fixed points vanishes,[3] which means that each element of $\mathrm{Fix}(\phi)$ has fixed point of multiplicity 1. But counting multiplicities, the total number of fixed points of a map of degree d is $d + 1 \geq 3$. (See, for example, [FG11, Appx. A].) This contradiction gives $\#T_\phi \geq 3$.

Finally, suppose that we are in the third case, so that $\mathrm{Fix}(\phi) = \{x\}$. We claim that $\#\phi^{-1}(x) \geq 2$. If not, x is ramified for ϕ, which implies that the derivative $\phi'(x)$ vanishes there. But the fact that x is the unique fixed point of ϕ means that in local coordinates centered at x our map is of the form

$$z \mapsto z + a_{d+1}z^{d+1} + \cdots \qquad \text{with } a_{d+1} \neq 0.$$

The derivative cannot vanish at x, and we must have $\#\phi^{-1}(x) \geq 2$ as desired. If $\phi^{-1}(x)$ consists of at least three points, then evidently so does $T_\phi = \phi^{-2}(x)$. Otherwise, $\phi^{-1}(x) = \{x, y\}$, which means that $T_\phi = \phi^{-2}(x) = \{x, y\} \cup \phi^{-1}(y)$, which satisfies $3 \leq \#T_\phi \leq d + 2$.

Define T_ϕ as in equation (4.1), and define T_ψ applying the same recipe to ψ. Write $E = F(T_\phi \cup T_\psi)$ for the field extension generated by the elements of $T_\phi \cup T_\psi$. Then $s(T_\phi) = T_\psi$ for every $s \in \mathrm{Conj}_{\phi,\psi}(E)$. We have therefore constructed an invariant pair.

4.2.3. *Descent.* While the greatest strength of the method of invariant sets lies in computing the absolute conjugating set, it can be adjusted to compute the conjugating set over a fixed ground field F. To use Algorithm 1 to compute $\mathrm{Conj}_{\phi,\psi}(F)$, we make the following modification. In the final step, after determining that $s \circ \phi = \psi \circ s$, we also check that the three points $s(0)$, $s(1)$, and $s(\infty)$ are defined over F. If so, then append s to the set L.

To see that this has the desired effect, we note that the element $s \in \mathrm{Conj}_{\phi,\psi}(E)$ is completely determined by its action on 3 distinct points of $\mathbb{P}^1(F)$. Moreover, if s maps three distinct F-rational points to three (distinct) F-rational points, then the system of linear equations determined by these 3 relations will have a solution over F. So $s \in \mathrm{Conj}_{\phi,\psi}(F)$, as desired.

To implement this strategy as an algorithm, we require an efficient method to detect if an element of a finite extension E/F lies in F (without computing the Galois group). We may represent E as an F vector space with basis $1, \alpha_1, \ldots, \alpha_n$, so that any element $\beta \in E$ may now be represented uniquely by a vector $c_0 + c_1\alpha_1 + \cdots + c_n\alpha_n$, where $c_i \in F$. The element β lies in F if and only if $c_1 = \cdots = c_{n-1} = 0$.

4.2.4. *Complexity.* The degree $d = \deg(\phi) = \deg(\psi)$ is the principle measure of complexity in this algorithm. If the coefficients of ϕ, ψ, and a candidate conjugating map $s \in \mathrm{PGL}_2(E)$ have length at most k bits, then verifying the equality $s \circ \phi = \psi \circ s$ requires $O(d^3k^2)$ bit operations in general. This can be reduced to $O(d^2 \log^3 q)$ if E is a finite field with q elements. The number of candidates $s \in \mathrm{PGL}_2(E)$ is approximately $\#T_\phi^3/6 = O(d^3)$, which can make this algorithm inefficient if the degree is large.

4.3. **Implementation Notes.** The main computational difficulty in implementation of this algorithm lies in performing operations in the field extension E. Typically, the invariant pairs described in Section 4.2.2 generate an extension of the field F of degree $(\deg(\phi) + 1)^2$. (It is $\deg(\phi) + 1$ when using this algorithm to compute the automorphism group.) In practice, if we only want the F-rational points of $\mathrm{Conj}_{\phi,\psi}$ or Aut_ϕ, then we can occasionally work with

[3] More precisely, the induced map $T\phi$ on the tangent space $T\mathbb{P}^1_x$ is zero.

a smaller field by building arithmetic considerations into the construction of the invariant pair. We do so by exploiting the following observation:

Lemma 4.1. *Fix an algebraic closure $\overline{F}$ and an invariant pair $T_\phi, T_\psi \subset \mathbb{P}^1(\overline{F})$. Then for any element $s \in \mathrm{Conj}_{\phi,\psi}(F)$ and any $\tau \in T_\phi$, we have $F(\tau) = F(s(\tau))$ and $s(\tau) \in T_\psi$. (Here we set $F(\infty) = F$.)*

Proof. Since $s \in \mathrm{Aut}_{\mathbb{P}^1}(F)$, any element of $\mathrm{Gal}(\overline{F}/F)$ fixes τ if and only if it fixes $s(\tau)$. Thus, by Galois theory, the two elements generate the same field. □

The lemma implies that we can modify Algorithm 1 and only consider triples of distinct integers i, j, k such that $F(\tau_i) = F(\eta_i)$. We carry this out as follows. We first construct T_ϕ as a union $T_{\phi,0} \cup T_{\phi,1} \cup \cdots \cup T_{\phi,r}$ where each $T_{\phi,i}$ is such that any 2 elements generate the same field extension, while any two elements from distinct $T_{\phi,i}$ do not generate the same field extension. We do the same for T_ψ. Renumbering if necessary, we may assume that $\#T_{\phi,i} \leq \#T_{\phi,i+1}$ and $\#T_{\psi,i} \leq \#T_{\psi,i+1}$ for all i. Moreover, we may assume that $F(T_{\phi,i}) = F(T_{\psi,i})$ for each i; if it is not possible to ensure these conditions, then $\mathrm{Conj}_{\phi,\psi}(F)$ is empty. Now select the smallest set of indices I such that the union $\cup_{i \in I} T_{\phi,i}$ contains at least 3 elements. Run Algorithm 1 with T_ϕ and T_ψ replaced by $\cup_{i\in I} T_{\phi,i}$ and $\cup_{i \in I} T_{\psi,i}$.

5. Algorithm 2: Chinese Remainder Theorem

Let K be a number field and suppose $\phi, \psi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ are morphisms of degree at least 2. In this section, we describe an algorithm to compute $\mathrm{Conj}_{\phi,\psi}(K)$ or $\mathrm{Aut}_\phi(K)$ that combines local and global arithmetic information.

Although this technique is limited to rational functions defined over number fields (or global function fields after appropriate modifications), it has the benefit of scaling well in practice as the degree grows, and it is particularly efficient at determining if the set $\mathrm{Conj}_{\phi,\psi}(K)$ is empty. However, if there exists a conjugating map (or automorphism) whose coefficients have moderately large height, then this algorithm may take quite a while to detect it. See the sample run times in §8.

5.1. **Overview.**

This algorithm uses an approach that is ubiquitous in number theory: first compute the conjugation set over the residue field $\mathbb{F}_v$ for some finite place(s) v, and then use the local information to obtain a global answer by applying a suitable form of the Chinese Remainder Theorem.

As a first step, we prove that for any invariant pair (as in §4.1) T_ϕ, T_ψ that is stable under the action of Galois, there exists a constant $C = C(K, \phi, \psi,)$ such that any element in $\mathrm{Conj}_{\phi,\psi}(K)$ has relative multiplicative height at most C (see Proposition 5.1). Thus we need only consider the finitely many elements of $\mathrm{Aut}_{\mathbb{P}^1}(K)$ of height at most C. Typically this height bound is much larger than necessary, so it is only used to ensure that our algorithm terminates.

We further restrict our search by considering only those conjugating elements that lie in congruence classes corresponding to elements of $\mathrm{Conj}_{\phi,\psi}(\mathbb{F}_v)$ at certain good places v of K, since Corollary 3.4 gives an injection $\mathrm{Conj}_{\phi,\psi}(K) \hookrightarrow \mathrm{Conj}_{\phi,\psi}(\mathbb{F}_v)$ for all but finitely many places. This local data can be computed first and then glued together using the Chinese Remainder Theorem to obtain global conjugating elements.

5.2. **Algorithm.** Pseudocode for the Chinese Remainder Theorem method is given in Algorithm 2. We first provide a proof of the height bound used in the algorithm, followed by a proof of correctness for the algorithm.

We use the following notation in the remainder of this section. (See, for example, [HS00, B.2, B.7] for number-theoretic definitions.)

- For any closed subset $T \subset \mathbb{P}^1(\overline{K})$, let $f_T \in K[w,z]_{(0)}$ be a homogeneous polynomial whose zero set is precisely T.
- Let $H_K\colon \mathbb{P}^1(K) \to \mathbb{R}_{\geq 1}$ denote the relative multiplicative height for K.
- Let $L_2(f)$ denote the L_2-norm of a polynomial f.
- Write $\mathcal{O}_K$ for the ring of integers of K, and write S for the finite set of places of $\mathcal{O}_K$ defined in Corollary 3.4. Then $\mathrm{Conj}_{\phi,\psi}(K) \hookrightarrow \mathrm{Conj}_{\phi,\psi}(\mathbb{F}_v)$ for each place v not in S.
- For a finite set of prime ideals $\mathfrak{p}_0, \ldots, \mathfrak{p}_n$ of $\mathcal{O}_K$ corresponding to places $v_0, \ldots, v_n$ not in S, we set $\mathfrak{a} = \prod_{0\leq i\leq n} \mathfrak{p}_i$ and $L = \bigcup_{0 \leq i \leq n} \mathrm{Conj}_{\phi,\psi}(\mathbb{F}_{v_j})$. Let $G \subseteq \mathrm{Aut}(\mathbb{P}^1_{\mathcal{O}_K/\mathfrak{a}})$ be a subset that surjects onto $\mathrm{Conj}_{\phi,\psi}(\mathbb{F}_{v_j})$ for each j. We write $G = \mathrm{CRT}(L)$.

Algorithm 2 — Computation of $\mathrm{Conj}_{\phi,\psi}(K)$ via the Chinese Remainder Theorem

```
Input: a number field $K$ and rational functions $\phi, \psi \in K(z)$ of degree $d \geq 2$
Output: the set $\mathrm{Conj}_{\phi,\psi}(K)$

choose an invariant pair $T_\phi, T_\psi$ as in Section 4.1
set $M = 6^{[K:\mathbb{Q}]} L_2(f_{T_\phi})^3 L_2(f_{T_\psi})^3$

create an empty list $L$, and set $\mathfrak{a} = \langle 1 \rangle$
for $v$ a prime of good reduction such that $\mathrm{Conj}_{\phi,\psi}(K) \to \mathrm{Conj}_{\phi,\psi}(\mathbb{F}_v)$ is injective:
  compute $\mathrm{Conj}_{\phi,\psi}(\mathbb{F}_v)$
  if $\mathrm{Conj}_{\phi,\psi}(\mathbb{F}_v) = \varnothing$:
    return $\varnothing$
  else:
    append $\mathrm{Conj}_{\phi,\psi}(\mathbb{F}_v)$ to L, and set $\mathfrak{a} = \mathfrak{a}\mathfrak{p}_v$
  set $G = \mathrm{CRT}(L)$ and initialize an empty list Conjs
  for $s$ in $G$:
    set $s' \in \mathrm{PGL}_2(\mathcal{O}_K)$ to be a lift of $s$ of minimal height
    if $H_K(s') \leq M$ and $s' \circ \phi = \psi \circ s'$:
      append $s'$ to Conjs
  if $\mathrm{N}(\mathfrak{a}) \geq 2^{[K:\mathbb{Q}]} M^2$ or if #Conjs = $\#\mathrm{Conj}_{\phi,\psi}(\mathbb{F}_v)$ for any $v \mid \mathfrak{a}$:
    return Conjs
```

5.2.1. *Height bounds for conjugating elements.*

Proposition 5.1. *Let $T, T' \subset \mathbb{P}^1(\overline{K})$ be Galois invariant sets of order at least* 3. *Then for any $s \in \mathrm{Aut}(\mathbb{P}^1_K) \subset \mathbb{P}^3(\overline{K})$ such that $s(T) = T'$, we have*

$$H_K(s) \leq 6^{[K:\mathbb{Q}]} L_2(f_T)^3 L_2(f_{T'})^3.$$

Remark 5.2. This bound is typically far from optimal. (For an example, see §5.3.)

Proof. Let s be as in the statement of the Proposition. Let τ_1, τ_2, τ_3 be 3 distinct elements of T, and let $\eta_i := s(\tau_i) \in T'$. In coordinates, we write $\tau_i = (\tau_{i,0} : \tau_{i,1})$ and $\eta_i = (\eta_{i,0} : \eta_{i,1})$. Since an automorphism of $\mathbb{P}^1$ is determined by its action on three elements, we have an expression for $s = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ in terms of $\tau_{i,j}, \eta_{i,j}$, i.e.,

$$\begin{aligned} \alpha &= \textstyle\sum_{\sigma \in S_3} (\mathrm{sgn}\ \sigma) B_{\sigma(1)} C_{\sigma(2)} D_{\sigma(3)}, & \beta &= \textstyle\sum_{\sigma \in S_3} (\mathrm{sgn}\ \sigma) A_{\sigma(1)} C_{\sigma(2)} D_{\sigma(3)}, \\ \gamma &= \textstyle\sum_{\sigma \in S_3} (\mathrm{sgn}\ \sigma) A_{\sigma(1)} B_{\sigma(2)} D_{\sigma(3)}, & \delta &= \textstyle\sum_{\sigma \in S_3} (\mathrm{sgn}\ \sigma) A_{\sigma(1)} B_{\sigma(2)} C_{\sigma(3)}, \end{aligned}$$

where $A_i = \tau_{i,0}\eta_{i,1}$, $B_i = -\tau_{i,1}\eta_{i,1}$, $C_i = -\tau_{i,0}\eta_{i,0}$, and $D_i = \tau_{i,1}\eta_{i,0}$.

This expression allows us to obtain a bound on the local height of s. Let v be any place of K and let $\varepsilon_v = 6$ if $v \mid \infty$ and $\varepsilon_v = 1$ if $v \nmid \infty$. Then, by the triangle inequality,

$$|\alpha|_v \leq \varepsilon_v \cdot \max_{\sigma \in S_3} |B_{\sigma(1)} C_{\sigma(2)} D_{\sigma(3)}|_v \leq \varepsilon_v \prod_{1 \leq i \leq 3} \max\{|\tau_{i0}|_v, |\tau_{i1}|_v\} \cdot \max\{|\eta_{i0}|_v, |\eta_{i1}|_v\}.$$

One can easily check that the same bound holds for $|\beta|_v, |\gamma|_v, |\delta|_v$. It follows that

$$\begin{aligned} H_K(s) &= \prod_v \max\{|\alpha|_v, |\beta|_v, |\gamma|_v, |\delta|_v\}^{[K_v:\mathbb{Q}_v]} \\ &\leq \prod_v \varepsilon_v^{[K_v:\mathbb{Q}_v]} \cdot \prod_{1 \leq i \leq 3} \max\{|\tau_{i0}|_v, |\tau_{i1}|_v\}^{[K_v:\mathbb{Q}_v]} \cdot \max\{|\eta_{i0}|_v, |\eta_{i1}|_v\}^{[K_v:\mathbb{Q}_v]} \\ &= 6^{[K:\mathbb{Q}]} \prod_{1 \leq i \leq 3} H_K(\tau_i) H_K(\eta_i). \end{aligned}$$

Since $H_K(\tau_i) \leq L_2(f_T)$ and $H_K(\eta_i) \leq L_2(f_{T'})$ [HS00, Lemma B.7.3.1], this completes the proof. □

Corollary 5.3. *Let $\phi, \psi \in K(z)$ be rational functions of degree ≥ 2, let $T_\phi, T_\psi \subset \mathbb{P}^1(\overline{K})$ be an invariant pair that is stable under the action of* $\mathrm{Gal}(\overline{K}/K)$.[4] *Then every element of* $\mathrm{Conj}_{\phi,\psi}(K)$*, viewed as an element of $\mathbb{P}^3(K)$, has relative multiplicative height bounded by* $6^{[K:\mathbb{Q}]} L_2(f_{T_\phi})^3 L_2(f_{T_\psi})^3$.

5.2.2. *Proof of correctness.* The correctness of Algorithm 2 is immediate from the next proposition.

Proposition 5.4. *Retain the notation and hypotheses of Proposition 5.1. Let $v_0, \ldots, v_n$ be finite places of K such that*

(1) *ϕ and ψ have good reduction at v_i for all i;*
(2) *the reduction map* $\mathrm{Conj}_{\phi,\psi}(K) \to \mathrm{Conj}_{\phi,\psi}(\mathbb{F}_{v_i})$ *is injective for all i; and*
(3) $\prod_i \mathrm{N}(v_i) \geq 2^{[K:\mathbb{Q}]} M^2$*, where* $M = 6^{[K:\mathbb{Q}]} L_2(f_{T_\phi})^3 L_2(f_{T_\psi})^3$.

For any tuple $(g_i) \in \prod_i \mathrm{Conj}_{\phi,\psi}(\mathbb{F}_{v_i})$*, let* $g_K \in \mathrm{Aut}(\mathbb{P}^1_K)$ *be a simultaneous lift of each g_i of minimal height. If* $(g_i) \in \mathrm{im}\big(\mathrm{Conj}_{\phi,\psi}(K) \to \prod_i \mathrm{Conj}_{\phi,\psi}(\mathbb{F}_{v_i})\big)$*, then* $g_K \in \mathrm{Conj}_{\phi,\psi}(K)$.

We first prove two lemmas.

Lemma 5.5. *Let $\mathfrak{b}$ be a nonzero fractional ideal of $\mathcal{O}_K$, and write it as a quotient $\mathfrak{b} = \mathfrak{b}^+/\mathfrak{b}^-$ of relatively prime integral ideals. Then $H_K(b) \geq \mathrm{N}(\mathfrak{b}^+)$ for all nonzero $b \in \mathfrak{b}$.*

[4] Observe that the invariant pairs constructed in §4.2.2 are Galois stable.

Proof. Since $b \in \mathfrak{b}$, we have $|b|_v \le 1$ for any finite place v such that $v(\mathfrak{b}) \ge 0$. Therefore

$$\begin{aligned} H_K(b) &= \prod_{v|\infty} \max\{1, |b|_v\}^{[K_v:\mathbb{Q}_v]} \prod_{\substack{v\nmid\infty \\ v(\mathfrak{b})<0}} \max\{1, |b|_v\}^{[K_v:\mathbb{Q}_v]} \\ &\ge \prod_{v|\infty} |b|_v^{[K_v:\mathbb{Q}_v]} \prod_{\substack{v\nmid\infty \\ v(\mathfrak{b})<0}} |b|_v^{[K_v:\mathbb{Q}_v]} = \prod_{\substack{v\nmid\infty \\ v(\mathfrak{b})\ge 0}} |b|_v^{-[K_v:\mathbb{Q}_v]}, \end{aligned}$$

where the last equality follows from the product formula. Let $e_{\mathfrak{p}}$ be such that $\mathfrak{b} = \prod \mathfrak{p}^{e_{\mathfrak{p}}}$. Since $b \in \mathfrak{b}$, we have $v(b) \ge e_{\mathfrak{p}_v}$. Hence $|b|_v^{-[K_v:\mathbb{Q}_v]} \ge \mathrm{N}(\mathfrak{p}_v)^{e_{\mathfrak{p}_v}}$. □

Lemma 5.6. *Let $\mathfrak{a} \subset \mathcal{O}_K$ be an integral ideal, and let $\rho_{\mathfrak{a}} \colon \mathbb{P}^n(\mathcal{O}_K) \to \mathbb{P}^n(\mathcal{O}_K/\mathfrak{a})$ denote the canonical projection. For each $b = (b_0 : b_1 : \cdots : b_n) \in \mathbb{P}^n(\mathcal{O}_K/\mathfrak{a})$, there is at most one element $a = (a_0 : a_1 : \cdots : a_n) \in \rho_{\mathfrak{a}}^{-1}(b)$ with $H_K(a) < \left(2^{-[K:\mathbb{Q}]}\mathrm{N}(\mathfrak{a})\right)^{1/2}$.*

Proof. Let $a, a' \in \mathbb{P}^n(\mathcal{O}_K)$ be such that $H_K(a), H_K(a') < \left(2^{-[K:\mathbb{Q}]}\mathrm{N}(\mathfrak{a})\right)^{1/2}$ and such that $\rho_{\mathfrak{a}}(a) = \rho_{\mathfrak{a}}(a')$. Since $a \in \mathbb{P}^n(\mathcal{O}_K)$, there exists a coordinate i_0 such that $a_{i_0} \notin \mathfrak{a}$. It follows that $a'_{i_0} \notin \mathfrak{a}$ too.

Then for each i and each place v, we have

$$\max\left\{1, \left|\frac{a_i}{a_{i_0}} - \frac{a'_i}{a'_{i_0}}\right|_v\right\} \le \varepsilon_v \max_{\ell}\left\{\left|\frac{a_\ell}{a_{i_0}}\right|_v\right\} \cdot \max_{\ell}\left\{\left|\frac{a'_\ell}{a'_{i_0}}\right|_v\right\},$$

where $\varepsilon_v = 1$ or 2 depending on whether v is non-Archimedean or Archimedean. Taking the product over all v gives $H_K\left(\frac{a_i}{a_{i_0}} - \frac{a'_i}{a'_{i_0}}\right) \le 2^{[K:\mathbb{Q}]} H_K(a) H_K(a')$. The latter is less than $\mathrm{N}(\mathfrak{a})$ by hypothesis, and $\frac{a_i}{a_{i_0}} - \frac{a'_i}{a'_{i_0}}$ lies in the fractional ideal $(a_{i_0}a'_{i_0})^{-1}\mathfrak{a}$, so the preceding lemma implies that $\frac{a_i}{a_{i_0}} = \frac{a'_i}{a'_{i_0}}$. That is, $a = a'$. □

Proof of Proposition 5.4. Assume that $(g_i) \in \operatorname{im}\left(\mathrm{Conj}_{\phi,\psi}(K) \to \prod_i \mathrm{Conj}_{\phi,\psi}(\mathbb{F}_{v_i})\right)$ and let $g' \in \mathrm{Conj}_{\phi,\psi}(K)$ denote its pre-image. Note that g' is unique by assumption (2). By Corollary 5.3,

$$H_K(g') \le M \le \left(2^{-[K:\mathbb{Q}]} \prod_i \mathrm{N}(v_i)\right)^{1/2}.$$

Applying Lemma 5.6 to the ideal $\mathfrak{a} = (\prod_i \mathrm{N}(v_i))$, we conclude that g' must have minimal height among all lifts, so $g' = g_K \in \mathrm{Conj}_{\phi,\psi}(K)$. □

5.3. **Implementation Notes.** When computing $\mathrm{Conj}_{\phi,\psi}(K)$, it is important to build in as many early termination conditions as possible, since typically the elements of $\mathrm{Conj}_{\phi,\psi}(K)$ have significantly smaller height than the theoretical bound M. This is of course true when $\mathrm{Conj}_{\phi,\psi}(K)$ is trivial, but it remains true even in the nontrivial case. For example, consider the function $\phi(z) = 345025251z^6 \in \mathbb{Q}(z)$. (See the last line of Table 3.) The height bound produced by Corollary 5.3 has over 50 digits, while, in contrast, the height of the unique nontrivial $\mathbb{Q}$-rational automorphism is 2601. The same phenomenon can be seen with many of the examples in Table 2.

5.3.1. *Conjugation sets.* In order to avoid extraneous computation, we want to detect as quickly as possible when two rational functions are *not* conjugate. The method of invariant sets suggests a useful criterion.

Let F be a field, let $a \in F \smallsetminus \{0\}$, let $f_1, \ldots, f_r \in F[X,Y]$ be pairwise coprime irreducible homogeneous polynomials, and let $e_1, \ldots, e_r \geq 1$ be integers. We define the **factorization type** (or simply **type**) of the polynomial $f := af_1^{e_1} \cdots f_r^{e_r}$ to be the multiset of pairs $\{(\deg(f_1), e_1), \cdots, (\deg(f_r), e_r)\}$. Note that the degree of f is determined by its type. The definition of type extends in the obvious way to inhomogeneous univariate polynomials.

Now suppose that $\phi, \psi \in F(z)$ are rational functions of degree $d \geq 2$ such that $\mathrm{Conj}_{\phi,\psi}(F)$ is nonempty. We saw in §4.2.2 that for each $s \in \mathrm{Conj}_{\phi,\psi}(F)$, we have $s(\mathrm{Fix}(\phi)) = \mathrm{Fix}(\psi)$. In fact, more is true. Write ϕ and ψ in homogeneous form as

$$\Phi = (\Phi_0(X,Y), \Phi_1(X,Y)) \quad \text{and} \quad \Psi = (\Psi_0(X,Y), \Psi_1(X,Y)).$$

The polynomials $f_\phi = X\Phi_1 - Y\Phi_0$ and $f_\psi = X\Psi_1 - Y\Psi_0$ determine the fixed points of ϕ and ψ, respectively. Writing s in homogeneous form as

$$S = (S_0(X,Y), S_1(X,Y)) = (\alpha X + \beta Y, \gamma X + \delta Y),$$

the condition $s \circ \phi \circ s^{-1} = \psi$ may be translated as $S \circ \Phi = \lambda \cdot \Psi \circ S$ for some $\lambda \in F^\times$. We now see that

$$\begin{aligned} \lambda f_\psi(S_0, S_1) &= \lambda\left[S_0 \cdot (\Psi_1 \circ S) - S_1 \cdot (\Psi_0 \circ S)\right] \\ &= S_0 \cdot (\gamma\Phi_0 + \delta\Phi_1) - S_1 \cdot (\alpha\Phi_0 + \beta\Phi_1) \\ &= (\alpha\delta - \beta\gamma)\,(X\Phi_1 - Y\Phi_0) = (\alpha\delta - \beta\gamma) f_\phi. \end{aligned} \tag{5.1}$$

Hence the types of f_ϕ and f_ψ agree. Said another way, if the types of the polynomials f_ϕ and f_ψ do not match, then $\mathrm{Conj}_{\phi,\psi}(F)$ is empty. Since $s(\phi^{-n}(\mathrm{Fix}(\phi))) = \psi^{-n}(\mathrm{Fix}(\psi))$ for every $n \geq 1$, a similar statement holds for the polynomials defining the n^{th} preimages of the fixed points.

Assume now that $F = \mathbb{F}_q$ is the finite field with q elements. By definition, the type of a homogeneous polynomial $f \in \mathbb{F}_q[X,Y]$ is computed by factoring it completely. However, there are well known "folk methods" for calculating the type of f. Using only formal derivatives and the Euclidean algorithm, one can determine the number of irreducible factors of a given degree and the exponents to which they occur in f. (See [CZ81, §2].)

If $F = K$ is a number field, then factoring f_ϕ and f_ψ may not be computationally efficient. An alternative approach is suggested by the Chinese Remainder Theorem method for computing $\mathrm{Conj}_{\phi,\psi}(K)$. Let v be a non-Archimedean place of K at which both ϕ and ψ have good reduction. Then each element of $\mathrm{Conj}_{\phi,\psi}(K)$ has good reduction at v, and we may reduce equation (5.1) modulo v to obtain a relation between the fixed point polynomials of ϕ_v and ψ_v, which are defined over the residue field $\mathbb{F}_v$. If $\mathrm{Conj}_{\phi,\psi}(K)$ is nonempty, then for each place of good reduction v for ϕ and ψ, the types of the polynomials f_ϕ and f_ψ must agree modulo v.[5] Algorithm 2 provides a collection of places v that are sufficient to compute the full set $\mathrm{Conj}_{\phi,\psi}(K)$ via the Chinese Remainder Theorem; one could use this set of places v for our early termination criterion as well.

[5] When f_ϕ and f_ψ are irreducible, it is equivalent to say that the splitting fields of f_ϕ and f_ψ have the same Dedekind zeta function [SP95]. One says that these splitting fields are "arithmetically equivalent."

5.3.2. *Automorphism groups.* In the case that $\phi = \psi$, the above early termination criteria will always fail since $\mathrm{Aut}_\phi(F)$ contains at least one element. In this case, one may instead use group-theoretic considerations as early termination criteria. These considerations can also be used in the CRT step, allowing us to avoid extraneous computation. We give an example here, and the curious reader can find more details in our source code.

Example 5.7. It is possible for the reduction of $\mathrm{Aut}_\phi(K)$ to be a proper subgroup of $\mathrm{Aut}_\phi(\mathbb{F}_v)$ for all places v of good reduction. Consider the rational function $\phi(z) = 2z^5$. One can use the method of invariant sets to check that

$$\mathrm{Aut}_\phi(\overline{\mathbb{Q}}) = \left\{z, iz, -z, -iz, (\sqrt{2}z)^{-1}, i(\sqrt{2}z)^{-1}, -(\sqrt{2}z)^{-1}, -i(\sqrt{2}z)^{-1}\right\},$$

which is a dihedral group of order 8. For all primes $p > 2$, at least one of $-1, 2, -2$ is a square in $\mathbb{F}_p$. Therefore, $\mathrm{Aut}_\phi(\mathbb{F}_p)$ always contains $\mathbb{Z}/2\times\mathbb{Z}/2$ or $\mathbb{Z}/4$ as a subgroup. As the algorithm is stated, we would compute a lift of every element in $\prod_{p=5}^{19} \mathrm{Aut}_\phi(\mathbb{F}_p)$. However, by $p = 7$ one can already recognize that $\mathrm{Aut}_\phi(\mathbb{Q}) \subseteq \mathbb{Z}/2$ since $\mathrm{Aut}_\phi(\mathbb{F}_5) = \mathbb{Z}/4$ and $\mathrm{Aut}_\phi(\mathbb{F}_7) = \mathbb{Z}/2\times\mathbb{Z}/2$. Our code checks for group-theoretic properties like this when deciding whether to terminate.

6. Algorithm 3: Method of Fixed Points

Let F be a field and let $\phi : \mathbb{P}^1_F \to \mathbb{P}^1_F$ be a morphism of degree $d \geq 2$. In this section we describe an algorithm to compute $\mathrm{Aut}_\phi(F)$ that capitalizes on a connection between fixed points of $s \in \mathrm{Aut}_\phi(F)$ and periodic points for ϕ of small period. This technique does not require working with points in an extension field of F, although it does require one to detect the linear and quadratic factors of univariate polynomials over F of degree $O(d^2)$. For this reason, it outperforms our other methods over finite fields, and over number fields when the degree is small. The CRT method is preferable for rational functions of larger degree over number fields. (See §8 for the empirical distinction between large and small degree in this context.)

6.1. **Overview.** A nontrivial element $s \in \mathrm{Aut}_\phi(F)$ has either one or two fixed points in $\mathbb{P}^1(\overline{F})$. If $x \in \mathrm{Fix}(s)$, we have

$$s(\phi(x)) = \phi(s(x)) = \phi(x). \tag{6.1}$$

So $\phi(x) \in \mathrm{Fix}(s)$, and $\mathrm{Fix}(s)$ consists of either one or two orbits for ϕ. From Proposition 2.4, we also have strong conditions on the order of $s \in \mathrm{Aut}_\phi(F)$. Combining these facts with an explicit change of coordinates on the fixed points of ϕ, we are able to conclude that a candidate s must be conjugate to either

$$\begin{pmatrix} \xi & 0 \\ 0 & 1 \end{pmatrix} \quad \text{for a root of unity } \xi \in F\left(\mathrm{Fix}(s)\right), \text{ or}$$

$$\begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} \quad \text{where } \lambda \in F \smallsetminus \{0\}.$$

(Here $F\left(\mathrm{Fix}(s)\right)$ indicates the field extension formed by adjoining the fixed points of s to F.) One can then loop over the finitely many possibilities for s and test if they are in $\mathrm{Aut}_\phi(\overline{F})$.

6.2. **Algorithm.** Pseudocode is given in Algorithm 3. Throughout, we assume that either F is finite, or that $\mathrm{char}(F) \nmid d(d-1)$. For any ϕ-periodic point $x \in \mathbb{P}^1(\overline{F})$, write $\mathrm{per}(x)$ for its exact period — i.e., the minimum positive integer i such that $\phi^i(x) = x$. If x is not periodic, write $\mathrm{per}(x) = +\infty$. For each pair of integers $i, j \in \{1, 2\}$, define the following set:

$$Z_{i,j} = \{x \in \mathbb{P}^1(\overline{F}) : \mathrm{per}(x) = i,\ [F(x) : F] = j\}. \tag{6.2}$$

We also define the following set of ordered pairs:

$$W = \{(x, y) : \phi(x) = x = \phi(y),\ [F(x) : F] = [F(y) : F] = 1\}. \tag{6.3}$$

Finally, we write $Z'_{1,2}$ for the subset of $Z_{1,2}$ consisting of points that generate an inseparable extension of F; evidently, it is necessary that $\mathrm{char}(F) = 2$ for $Z'_{1,2}$ to be nonempty.

These sets may be constructed by extracting the linear and quadratic factors of the polynomials that define the fixed points of ϕ, the points of period 2, and the preimages of F-rational fixed points. We write $Z^{(2)}$ for the set of unordered pairs of elements of a set Z.

6.2.1. *Proof of correctness.* It is clear that the output of Algorithm 3 is contained in $\mathrm{Aut}_\phi(F)$ and contains the identity. It remains to prove that Algorithm 3 finds every nontrivial element of $\mathrm{Aut}_\phi(F)$.

Let $s = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ be a nontrivial element of $\mathrm{Aut}_\phi(F)$. The homogeneous polynomial defining the fixed points of s is $\gamma X^2 + (\delta - \alpha)XY - \beta Y^2$. In particular, s has either one or two distinct fixed points.

Case 1: Two fixed points. Suppose that $s \in \mathrm{Aut}_\phi(F)$ has two distinct fixed points, x_1 and x_2. From equation (6.1), we have $\phi(x_1), \phi(x_2) \in \{x_1, x_2\}$. There are three possible cases:

(1) ϕ fixes both x_1 and x_2;
(2) ϕ swaps x_1 and x_2; or
(3) $\phi(x_1) = x_2$ and ϕ fixes x_2 (perhaps after interchanging x_1 and x_2).

Since ϕ is defined over F, the Galois conjugates of a fixed point must also be fixed points. Thus in cases (1) and (2), either x_1 and x_2 are both F-rational, or they are quadratic conjugates over F. In case (3), both x_1 and x_2 must be F-rational.

Now suppose that x_1 and x_2 are both F-rational in case (1) — i.e., that $(x_1, x_2) \in Z^{(2)}_{1,1}$. Then we may select $u \in \mathrm{PGL}_2(F)$ such that $u(x_1) = \infty$ and $u(x_2) = 0$. In this case,

$$s = u^{-1} \begin{pmatrix} \zeta & 0 \\ 0 & 1 \end{pmatrix} u \quad \text{for some root of unity } \zeta \in F.$$

If ζ has order n, then n divides one of d, $d+1$, or $d-1$ by Proposition 2.4. Therefore, s will be found by the first for–loop of the algorithm with $S = Z^{(2)}_{1,1}$.

Similarly, if s falls in case (2) with x_1, x_2 F-rational, or in case (3), then s will be found in the part of the first for–loop corresponding to $S = Z^{(2)}_{2,1}$ and $S = W$, respectively.

For the case where x_1, x_2 are quadratic conjugates, we will use the following lemma.

Lemma 6.1. *Let $z_1, z_2 \in \overline{F}$ be quadratic conjugates. Fix $u \in \mathrm{PGL}_2(\overline{F})$ so that $u(z_1) = 0$ and $u(z_2) = \infty$, and let $\xi \in \overline{F}$. Then*

$$s := u^{-1} \begin{pmatrix} \xi & 0 \\ 0 & 1 \end{pmatrix} u$$

Algorithm 3 — Computation of $\mathrm{Aut}_\phi(F)$ via the method of fixed points

```
Input: a field $F$ and $\phi \in F(z)$ of degree $\geq 2$
Output: the set $\mathrm{Aut}_\phi(F)$

create a list $T$ of $F$-rational roots of $C_i(X) := X^{d+i} - 1$ for $i = -1, 0, 1$
create a list $\Lambda$ containing $-1$ and roots of $F$-quadratic factors of $C_i(X)$ for $i = -1, 0, 1$

create a list $L = [z]$
create the sets $Z_{i,j}, W$ defined in equations (6.2) and (6.3)

for each set $S$ among $Z_{1,1}^{(2)}$, $Z_{2,1}^{(2)}$, and $W$:
  for each pair $(x, y)$ with $x \neq y$ in $S$:
    choose $u \in \mathrm{PGL}_2(F)$ such that $u(x) = \infty$ and $u(y) = 0$
    for $\zeta \in T \smallsetminus \{1\}$:
      set $s(z) = u^{-1}(\zeta u(z))$
      if $s \circ \phi = \phi \circ s$: append $s$ to $L$

for each set $S$ among $(Z_{1,2} \smallsetminus Z_{1,1})$ and $(Z_{2,2} \smallsetminus Z_{2,1})$:
  for each element $x$ in $S$:
    set $y$ to be the Galois conjugate of $x$
    choose $u \in \mathrm{PGL}_2(F(x, y))$ such that $u(x) = \infty$ and $u(y) = 0$
    for $\xi \in \Lambda$:
      set $s(z) = u^{-1}(\xi u(z))$
      if $s \circ \phi = \phi \circ s$: append $s$ to $L$

if $p \nmid d(d-1)$ or $\# \mathrm{Fix}(\phi) \not\equiv 1 \pmod{p}$ or ($\# \mathrm{Fix}(\phi) = 1$ and $\# \phi^{-1}(\mathrm{Fix}(\phi)) \not\equiv 1 \pmod{p}$):
  return $L$

if $\# \mathrm{Fix}(\phi) > 1$: set $T = \mathrm{Fix}(\phi)$
else: set $T = \phi^{-1}(\mathrm{Fix}(\phi))$

for $x \in Z_{1,1} \cup Z'_{1,2}$:
  set $F' = F(x)$
  choose $u \in \mathrm{PGL}_2(F')$ such that $u(x) = \infty$
  choose $y_1 \in T \smallsetminus \{x\}$
  for $y_2 \in T \smallsetminus \{x, y_1\}$, $y_2 \in F'(y_1)$:
    set $\lambda = u(y_2) - u(y_1)$
    if $s(z) := u^{-1}(u(z) + \lambda)$ lies in $\mathrm{PGL}_2(F)$ and satisfies $s \circ \phi = \phi \circ s$:
      append $s$ to $L$

return $L$
```

defines a nontrivial finite-order element of $\mathrm{PGL}_2(F)$ *if and only if* $\xi = -1$ *and* $\mathrm{char}(F) \neq 2$, *or* $F(\xi) = F(z_1)$ *and* ξ *is a root of unity.*

Proof. The element s is independent of our choice of u, so we may set $u := \left(\begin{smallmatrix} 1 & -z_1 \\ 1 & -z_2 \end{smallmatrix}\right)$. Then

$$s = u^{-1} \begin{pmatrix} \xi & 0 \\ 0 & 1 \end{pmatrix} u = \begin{pmatrix} z_1 - \xi z_2 & (\xi - 1) z_1 z_2 \\ 1 - \xi & \xi z_1 - z_2 \end{pmatrix}, \tag{6.4}$$

which is of order n if and only if ξ is an n^{th} root of unity. (We neglect the determinant $z_2 - z_1$ of u because the computation occurs in PGL_2.) Write $F' = F(z_1) = F(z_2)$. The element s is defined over F if and only if $\xi \in F'$ and the nontrivial element σ of $\mathrm{Gal}(F'/F)$ fixes $\frac{z_1 - \xi z_2}{1-\xi}$ and $\frac{z_2 - \xi z_1}{1-\xi}$. By expanding the resulting equations and noting that $\sigma(z_1) = z_2$, we see that this happens if and only if $\xi\xi^\sigma = 1$, which completes the proof. □

Returning to our setup, we suppose that $s \in \mathrm{Aut}_\phi(F)$ and $\mathrm{Fix}(s) = \{x_1, x_2\}$ with x_1 and x_2 quadratic Galois conjugates. If $x_1, x_2 \in Z_{1,2} \smallsetminus Z_{1,1}$ (case (1)) or if $x_1, x_2 \in Z_{2,2} \smallsetminus Z_{1,2}$ (case (2)), then the lemma shows that s will be detected by the second for–loop of Algorithm 3. This completes the proof when s has two distinct fixed points.

Case 2: One fixed point. Assume that $s \in \mathrm{PGL}_2(F)$ has a unique fixed point x. Then F is a field of characteristic $p > 0$ and s has order p. (Move the unique fixed point to infinity. Then s is a nontrivial translation with finite order.) The proof of Proposition 2.4 shows that $p = \mathrm{ord}(s) | d(d-1)$. Now

$$s(\phi(x)) = \phi(s(x)) = \phi(x), \text{ so that } \phi(x) = x.$$

In addition, the group generated by s permutes the fixed points of ϕ, so that $\mathrm{Fix}(\phi) \smallsetminus \{x\}$ breaks up into disjoint orbits of size p. It follows that $\#\,\mathrm{Fix}(\phi) \equiv 1 \pmod{p}$. A similar argument shows that the group generated by s acts on the set $\phi^{-1}(\mathrm{Fix}(\phi))$. As x lies in this set, it must also have cardinality congruent to $1 \pmod{p}$. This justifies the early termination criterion in the middle of Algorithm 3.

Let $F' = F(x)$. As x is the unique solution of the fixed point equation for s, we have $F' = F$ or $\mathrm{char}(F) = 2$ and F' is a quadratic inseparable extensions of F. Select $u \in \mathrm{PGL}_2(F')$ such that $u(x) = \infty$. Then

$$usu^{-1} = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}, \qquad \text{where } \lambda \in F'.$$

If $\#\,\mathrm{Fix}(\phi) > 1$, let $y_1 \in \mathrm{Fix}(\phi) \smallsetminus \{x\}$, and set $y_2 := s(y_1)$. Then $u(y_2) - u(y_1) = \lambda$. It follows that

$$s(z) = u^{-1} \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix} u(z) = u^{-1}\left(u(z) + \lambda\right).$$

Thus, the third for-loop of Algorithm 3 finds s. Note that, in order to determine if s is defined over the field F, we can use the descent technique described in §4.2.3.

If instead $\#\,\mathrm{Fix}(\phi) = 1$, then we may use the same argument as in the previous paragraph with $y_1, y_2 \in \phi^{-1}(x) \smallsetminus \{x\}$. (By arguments in §4.2.2, $\#\phi^{-1}(x) > 1$). This completes the proof that every $s \in \mathrm{PGL}_2(F)$ is correctly found by Algorithm 3.

6.3. **Implementation Notes.** In our implementation over $\mathbb{Q}$, the main bottleneck in the method of fixed points lies in computing $Z_{1,2}$ and $Z_{2,2}$, which requires finding the quadratic factors of a degree $d^2 + 1$ polynomial. Our approach is to factor this polynomial completely and then read off the quadratic factors. It would be advantageous for the method of fixed points to give a more direct technique for computing these factors.

Our implementation over finite fields does not suffer from this drawback as there are efficient techniques for computing quadratic factors in this setting. See, e.g., [CZ81]. (Note that the method of fixed points over finite fields is used as an intermediate step in the CRT method over number fields.)

7. Naive algorithms

Each of the three algorithms described in Sections 4–6 takes advantage of some dynamical structure in order to compute either $\mathrm{Conj}_{\phi,\psi}(F)$ or $\mathrm{Aut}_{\phi}(F)$. It is worth noting that at least two algorithms could be implemented that make no use of the dynamical structure at all. In this section, we briefly describe these two algorithms.

7.1. **Gröbner bases.** Buchberger's algorithm allows one to compute the points of a zero-dimensional scheme by constructing a Gröbner basis for its ideal of definition I with respect to an appropriate monomial ordering [Eis95, Ch. 15]. Roughly, this is akin to performing Gaussian elimination in a nonlinear setting. Over a fixed polynomial ring, its performance typically degrades as the degrees of the generators of I grow. When $d = \deg(\phi) = \deg(\psi)$, we saw in §3 that $\mathrm{Conj}_{\phi,\psi}$ is a zero-dimensional scheme, naturally defined by $2d+1$ homogeneous polynomials of degree $d+1$ in four variables, and so this method may be readily applied.

7.2. **Finite fields — Exhaustive search.** Writing $\mathbb{F}_q$ for the finite field with q elements, one sees that $\mathrm{PGL}_2(\mathbb{F}_q)$ contains $q(q^2-1)$ elements. When q and d are small, it is reasonably efficient to compute $\mathrm{Conj}_{\phi,\psi}(\mathbb{F}_q)$ by exhaustive search. Indeed, verifying the identity $\psi \circ s = s \circ \phi$ requires $O(d^2 \log^3 q)$ bit operations for a general choice of ϕ and ψ of degree d and an element $s \in \mathrm{PGL}_2(\mathbb{F}_q)$. Since we expect $\mathrm{Conj}_{\phi,\psi}(\mathbb{F}_q)$ is empty, this method typically requires $O(q^3)$ such verifications to complete. When $\phi = \psi$, so that $\mathrm{Conj}_{\phi,\psi}(\mathbb{F}_q) = \mathrm{Aut}_{\phi}(\mathbb{F}_q)$, this approach can be accelerated by using the classification of subgroups of $\mathrm{PGL}_2(\mathbb{F}_q)$ [Fab12, Thm. D] to build in early termination conditions.

8. Comparison of algorithms over $\mathbb{Q}$

8.1. **Overview.** This table summarizes the algorithms being compared, and what they are designed to compute.

Algorithm	**Abbreviation**	**Computes**
Method of invariant sets (§4)	IS	$\mathrm{Conj}_{\phi,\psi}(\overline{F})$ for arbitrary field F
Chinese Remainder Theorem (§5)	CRT	$\mathrm{Conj}_{\phi,\psi}(K)$ for number field K
Method of fixed points (§6)	FP	$\mathrm{Aut}_{\phi}(F)$ for arbitrary field F
Gröbner Bases (§7)	GB	$\mathrm{Conj}_{\phi,\psi}(F)$ for arbitrary field F

Since the method of fixed points can only be applied to the computation of $\mathrm{Aut}_{\phi}(\mathbb{Q})$ and not $\mathrm{Conj}_{\phi,\psi}(\mathbb{Q})$, we restrict to computing automorphisms for comparison purposes. We implemented each of our algorithms in Sage to facilitate this comparison.

First, we present median running times for randomly generated rational functions of varying degrees and varying heights (Table 1). All of these randomly generated functions had trivial automorphism group. We did not include the running times of the Gröbner basis method when $d > 9$ since it is already apparent that this method was no longer competitive. We also did not include the method of invariant sets in this table, as it was not at all competitive with the others. For a random function of degree d, the fixed points likely generate an S_{d+1} extension of $\mathbb{Q}$, which requires working over a large degree number field, causing a dramatic slowdown in the method of invariant sets.

Next, as an approximation of "random" rational functions with nontrivial automorphism group, we compute the automorphism group of conjugates of z^k, where the conjugating functions were chosen randomly (Table 2). Finally, we present some hand-selected examples with nontrivial automorphism group which demonstrate the correctness of the algorithms (Table 3).

These examples were computed on a Macbook Pro (Apple, Inc.) running Mac OS X 10.9.1 with a 2.4 GHz Intel Core i5 processor and 16GB of RAM. The fixed point method, CRT method, and invariant sets method were run with Sage 6.0 which was released on December 17, 2013. The Gröbner basis method was run with `Magma` V2.19-10.[6]

All running times are listed in seconds.

8.2. **Performance comparisons.** The relative performance of the algorithms depends on the height and degree of the rational function in question, as well as on the existence of nontrivial automorphisms over the desired ground field and over an algebraic closure.

8.2.1. *Functions with trivial automorphism group.* If the rational function in question is "random," then it is likely to have trivial automorphism group. In this case, our computations indicate that the method of fixed points is preferable for functions of degree less than 10, while the CRT method gains an advantage for functions of large degree. The Gröbner basis method stays competitive for very small degrees ($d \approx 3$), but quickly lags behind. We also note that the height of the rational function seems to have a great effect on the Gröbner basis method. This is in stark contrast to the fixed point and CRT methods, where there is no discernible dependence on the height. The method of invariant sets is never competitive, regardless of the degree; this is unsurprising as we expect it to require working over an S_{d+1} extension of $\mathbb{Q}$.

8.2.2. *Functions with nontrivial automorphism group.* In the presence of a nontrivial automorphism, the performance of the CRT method becomes much more variable due in part to the increased difficulty of finding early terminating conditions. The method of invariant sets performs better in this case than in the previous case, mostly because a nontrivial automorphism usually forces the invariant sets to break into Galois orbits of smaller cardinality, which allows us to work over a smaller field.

Overall, the fixed point method performs the best. The method of invariant sets and, when the degree is small the Gröbner basis method, are occasionally comparable.

[6] It is possible that the running time gap between our algorithms and the "naive" Gröbner basis algorithm is partly due to this difference is programs; however, the gap is so large that we believe it cannot possibly account for all of the difference.

d		Height Bound					
		50	10^2	10^3	10^4	10^5	10^6
3	**FP**	0.003	0.003	0.003	0.003	0.003	0.003
	CRT	0.02	0.02	0.01	0.02	0.02	0.02
	GB	0.01	0.01	0.01	0.01	0.01	0.01
6	**FP**	0.008	0.008	0.009	0.009	0.009	0.01
	CRT	0.009	0.02	0.04	0.02	0.03	0.02
	GB	0.31	0.42	0.56	0.77	1.02	1.28
9	**FP**	0.03	0.03	0.03	0.03	0.03	0.03
	CRT	0.04	0.04	0.04	0.04	0.04	0.04
	GB	2.10	2.36	3.15	4.24	5.22	6.35
12	FP	0.10	0.11	0.11	0.11	0.11	0.12
	CRT	0.06	0.07	0.07	0.06	0.07	0.07
15	FP	0.35	0.35	0.34	0.35	0.37	0.37
	CRT	0.13	0.11	0.10	0.13	0.12	0.12
18	FP	0.97	0.95	0.97	0.99	0.98	1.01
	CRT	0.27	0.29	0.26	0.25	0.22	0.26
21	FP	2.23	2.34	2.26	2.32	2.39	2.39
	CRT	0.42	0.45	0.47	0.48	0.44	0.45

Table 1. Median running times for the three algorithms on 100 random rational functions with given degree and height bound.

k	f	FP	CRT	IS	GB	$\mathrm{Aut}_{\phi^f}(\mathbb{Q})$
3	$\frac{3z-7}{5z-1}$	**0.01**	1.78	0.03	**0.01**	$z, \frac{z+5}{3z-1}, \frac{-19z+21}{-5z+19}, \frac{11z-29}{13z-11}$
-3	$\frac{-3z}{-3z-4}$	**0.01**	2.60	0.05	0.02	$z, \frac{z}{2z-1}, \frac{-9z+9}{7z+9}, \frac{-9z+9}{-25z+9}$
6	$\frac{7z+10}{-3z+8}$	0.03	1.10	**0.02**	0.16	$z, \frac{101z-51}{55z-101}$
-6	$\frac{-7z-7}{-3z+1}$	**0.02**	0.04	0.12	0.22	$z, \frac{7z}{4z-7}$
9	$\frac{z-8}{4z-10}$	**0.08**	27.31	0.25	2.21	$z, \frac{84z-65}{116z-84}, \frac{-21z+8}{-40z+21}, \frac{-76z+63}{-84z+76}$
-9	$\frac{8z+1}{-2z+9}$	**0.06**	30.14	0.93	9.05	$z, \frac{25z+63}{77z-25}, \frac{-35z+8}{18z+35}, \frac{7z+65}{-85z-7}$
12	$\frac{-2z-10}{4z+1}$	0.11	0.19	**0.02**	16.81	$z, \frac{-2z-96}{-15z+2}$
-12	$\frac{-3z}{-5z+1}$	**0.17**	0.19	1.64	11.54	$z, \frac{5z-3}{8z-5}$
15	$\frac{z+9}{-z+1}$	0.36	4.51	**0.05**	83.18	$z, -z+8, \frac{4z+9}{z-4}, \frac{4z-41}{z-4}$
-15	$\frac{-4z-1}{8z-8}$	1.85	11.49	**0.18**	243.56	$z, -z-\frac{3}{8}, \frac{-3z+1}{16z+3}, \frac{-24z-17}{128z+24}$
18	$\frac{z+10}{5z+10}$	1.45	1.66	**0.04**	373.77	$z, \frac{95z-99}{75z-95}$
-18	$\frac{1}{3}(2z-5)$	**0.63**	0.95	2.65	29.8	$z, \frac{-5z-7}{3z+5}$

TABLE 2. Running times on ϕ^f where $\phi(z) = z^k$. Automorphism groups are either $\mathbb{Z}/2$ or $\mathbb{Z}/2 \times \mathbb{Z}/2$.

ϕ	FP	CRT	IS	GB	$\mathrm{Aut}_{\phi}(\mathbb{Q})$	group
$\frac{z^2-2z-2}{-2z^2-2z+1}$	0.03	0.32	0.03	**0.02**	$z^{\pm 1}, \left(\frac{-z}{z+1}\right)^{\pm 1}, (-z-1)^{\pm 1}$	$\mathfrak{D}_6$
$\frac{z^2+2z}{-2z-1}$	**0.01**	0.04	**0.01**	0.02	$z^{\pm 1}, \left(\frac{-z}{z+1}\right)^{\pm 1}, (-z-1)^{\pm 1}$	$\mathfrak{D}_6$
$\frac{z^2-4z-3}{-3z^2-2z+2}$	**0.01**	0.02	0.09	**0.01**	$z, \frac{-z-1}{z}, \frac{-1}{z+1}$	$\mathfrak{C}_3$
$\frac{z^5+5z^4-20z^3+10z^2+5z-2}{2z^5-5z^4-10z^3+20z^2-5z-1}$	**0.02**	0.18	0.08	0.08	$z, -z+1, \frac{1}{z}, \frac{z}{z-1}, \frac{2z-1}{z-2}, \frac{-z+2}{z+1},$ $\frac{z+1}{2z-1}, \frac{z-2}{2z-1}, \frac{-1}{z-1}, \frac{z-1}{z}, \frac{-z-1}{z-2}, \frac{2z-1}{z+1}$	$\mathfrak{D}_{12}$
$\frac{z^5-5z^4+10z^2-5z}{-5z^4+10z^3-5z+1}$	**0.02**	0.70	0.12	0.07	$z, \frac{z}{z-1}, -z+1, \frac{1}{z}, \frac{2z-1}{z-2}, \frac{-z+2}{z+1},$ $\frac{z-2}{2z-1}, \frac{z+1}{2z-1}, \frac{-1}{z-1}, \frac{z-1}{z}, \frac{-z-1}{z-2}, \frac{2z-1}{z+1}$	$\mathfrak{D}_{12}$
$\frac{z^5-20z^4+30z^3+10z^2-20z+3}{-3z^5-5z^4+40z^3-30z^2-5z+4}$	**0.01**	0.17	4.06	0.12	$z, \frac{z-2}{2z-1}, \frac{-1}{z-1}, \frac{z-1}{z}, \frac{-z-1}{z-2}, \frac{2z-1}{z+1}$	$\mathfrak{C}_6$
$\frac{3z^2-1}{z^3-3z}$	**0.02**	0.06	0.07	**0.02**	$\pm z, \pm\frac{1}{z}, \pm\left(\frac{-z+1}{z+1}\right), \pm\left(\frac{z+1}{z-1}\right)$	$\mathfrak{D}_8$
$\frac{z^3-3z}{-3z^2+1}$	**0.01**	0.05	0.02	0.02	$\pm z, \pm\frac{1}{z}, \pm\left(\frac{-z+1}{z+1}\right), \pm\left(\frac{z+1}{z-1}\right)$	$\mathfrak{D}_8$
$\frac{z^3-21z^2-3z+7}{-7z^3-3z^2+21z+1}$	**0.01**	0.15	0.38	0.02	$z, \frac{-1}{z}, \frac{z-1}{z+1}, \frac{-z-1}{z-1}$	$\mathfrak{C}_4$
$\frac{z^{11}+66z^6-11z}{-11z^{10}-66z^5+1}$	**0.02**	0.09	0.09	0.30	$z, -1/z$	$\mathfrak{C}_2$
$345025251z^6$	**0.01**	122.05	**0.01**	0.06	$z, 1/(2601z)$	$\mathfrak{C}_2$

TABLE 3. Running times on rational functions with nontrivial automorphism group.

References

[BR10] Matthew Baker and Robert Rumely, *Potential theory and dynamics on the Berkovich projective line*, Mathematical Surveys and Monographs, vol. 159, American Mathematical Society, Providence, RI, 2010. MR MR2599526

[CZ81] David G. Cantor and Hans Zassenhaus, *A new algorithm for factoring polynomials over finite fields*, Math. Comp. **36** (1981), no. 154, 587–592. MR 606517 (82e:12020)

[Eis95] David Eisenbud, *Commutative algebra*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995, With a view toward algebraic geometry. MR 1322960 (97a:13001)

[Fab12] Xander Faber, *Finite p-irregular subgroups of* $\mathrm{PGL}_2(k)$, Preprint, arXiv:1112.1999v2 [math.NT], 2012.

[Fab13] ———, *Topology and geometry of the Berkovich ramification locus for rational functions, I*, Manuscripta Math. **142** (2013), no. 3-4, 439–474. MR 3117171

[FG11] Xander Faber and Andrew Granville, *Prime factors of dynamical sequences*, J. Reine Angew. Math. **661** (2011), 189–214. MR 2863906

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52. MR MR0463157 (57 #3116)

[HS00] Marc Hindry and Joseph H. Silverman, *Diophantine geometry. an introduction*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000. MR MR1745599 (2001e:11058)

[LMT12] Alon Levy, Michelle Manes, and Bianca Thompson, *Uniform bounds for preperiodic points in families of twists*, Preprint, arXiv:1204.4447 [math.NT], 2012.

[Mil93] John Milnor, *Geometry and dynamics of quadratic rational maps*, Experiment. Math. **2** (1993), no. 1, 37–83, With an appendix by the author and Lei Tan. MR 1246482 (96b:58094)

[Mil09] ———, *Cubic polynomial maps with periodic critical orbit. I*, Complex dynamics, A K Peters, Wellesley, MA, 2009, pp. 333–411.

[Poo98] Bjorn Poonen, *The classification of rational preperiodic points of quadratic polynomials over* $\mathbf{Q}$*: a refined conjecture*, Math. Z. **228** (1998), no. 1, 11–29. MR 1617987 (99j:11076)

[PST09] Clayton Petsche, Lucien Szpiro, and Michael Tepper, *Isotriviality is equivalent to potential good reduction for endomorphisms of* $\mathbb{P}^N$ *over function fields*, J. Algebra **322** (2009), no. 9, 3345–3365. MR 2567424

[RL05] Juan Rivera-Letelier, *Points périodiques des fonctions rationnelles dans l'espace hyperbolique p-adique*, Comment. Math. Helv. **80** (2005), no. 3, 593–629. MR 2165204 (2006d:37081)

[Sil07] Joseph H. Silverman, *The arithmetic of dynamical systems*, Graduate Texts in Mathematics, vol. 241, Springer, New York, 2007. MR MR2316407

[Sil09] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094 (2010i:11005)

[SP95] D. Stuart and R. Perlis, *A new characterization of arithmetic equivalence*, J. Number Theory **53** (1995), no. 2, 300–308. MR 1348765 (96e:11151)

Department of Mathematics, University of Hawaii at Manoa, Honolulu, HI
E-mail address: xander@math.hawaii.edu, mmanes@math.hawaii.edu

Department of Mathematics, Brown University, Providence, RI
E-mail address: bviray@math.brown.edu